(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 June 2005 (16.06.2005)

PCT

(10) International Publication Number
WO 2005/055073 A1

(51) International Patent Classification[7]: G06F 15/18

(21) International Application Number:
PCT/GB2004/004919

(22) International Filing Date:
22 November 2004 (22.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

0327612.8	27 November 2003 (27.11.2003)	GB
0327627.6	28 November 2003 (28.11.2003)	GB
0424076.8	1 November 2004 (01.11.2004)	GB

(71) Applicant *(for all designated States except US)*: **QINETIQ LIMITED** [GB/GB]; Registered Office, 85 Buckingham Gate, London SW1 6PD (GB).

(72) Inventors; and

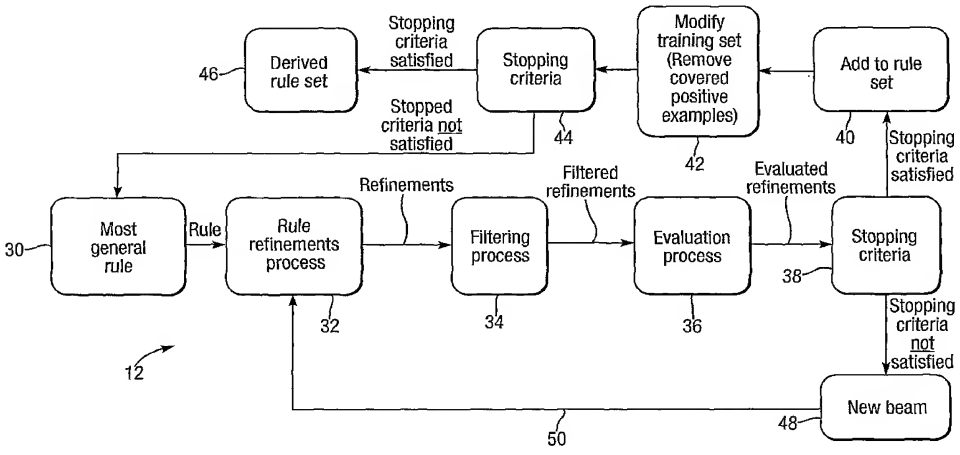
(75) Inventors/Applicants *(for US only)*: **LOCK, Zoe, Paula** [GB/GB]; QinetiQ Limited, Malvern Technology Centre, St Andrews Road, Malvern, Worcs WR14 3PS (GB). **PEELING, Emma, Cecilia** [GB/GB]; QinetiQ Limited, Malvern Technology Centre, St Andrews Road, Malvern, Worcs WR14 3PS (GB). **THIE, Claire, Julia** [GB/GB]; QinetiQ Limited, Malvern Technology Centre, St Andrews Road, Malvern, Worcs WR14 3PS (GB). **BROWN, Neil, Christopher, Charles** [GB/GB]; QinetiQ Limited, Malvern Technology Centre, St Andrews Road, Malvern, Worcs WR14 3PS (GB). **HATCH, Richard** [GB/GB]; QinetiQ Limited, Malvern Technology Centre, St Andrews Road, Malvern, Worcs WR14 3PS (GB). **HOOD, Alan, Barry** [GB/GB]; QinetiQ Limited, Malvern Technology Centre, St Andrews Road, Malvern, Worcs WR14 3PS (GB). **KILVINGTON, Simon** [GB/GB]; QinetiQ Limited, Malvern Technology Centre, St Andrews Road, Malvern, Worcs WR14 3PS (GB). **ZAKIUDDIN, Mohammed, Irfan** [GB/GB]; QinetiQ Limited, Malvern Technology Centre, St Andrews Road, Malvern, Worcs WR14 3PS (GB).

(74) Agent: **WILLIAMS, A., W., S.**; QinetiQ Ltd, IP Formalities, Cody Technology Park, A4 Building, Room G016, Ively Road, Farnborough, Hampshire GU14 0LX (GB).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN,

[Continued on next page]

(54) Title: AUTOMATED ANOMALY DETECTION



(57) Abstract: A method of anomaly detection applicable to telecommunications or retail fraud or software vulnerabilities uses inductive logic programming to develop anomaly characterisation rules from relevant background knowledge and a training data set, which includes positive anomaly samples of data covered by rules. Data samples include 1 or 0 indicating association or otherwise with anomalies. An anomaly is detected by a rule having condition set which the anomaly fu,lfils. Rules are developed by addition of conditions and unification of variables, and are filtered to remove duplicates, equivalents, symmetric rules and unnecessary conditions. Overfitting of noisy data is avoided by an encoding cost criterion. Termination of rule construction involves criteria of rule length, absence of negative examples, rule significance and accuracy, and absence of recent refinement. Iteration of rule construction involves selecting rules with unterminated construction, selecting rule refinements associated with high accuracies, and iterating a rule refinement, filtering and evaluation procedure (32 to 38) to identify any refined rule usable to test data. Rule development may use first order logic or Higher Order logic.

WO 2005/055073 A1

CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.